Elliptic Pairs and Elliptic Reciprocity

Liljana Babinkostova[1], Kevin Bombardier[2], Matthew Cole[3], Thomas Morrell[4], and Cory Scott[5]

[1]Boise State University, [2]Wichita State University, [3]University of Notre Dame, [4]Washington University in St. Louis, [5]Colorado College

Elliptic Curves and the Group Law

An elliptic curve is a non-singular (smooth) cubic

$$E : y^2 = x^3 + Ax + B,$$

either defined geometrically in the projective plane $\mathbb{P}^2$, or else defined algebraically over a field K.

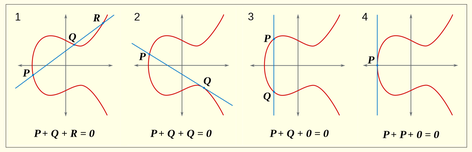

Figure 1: Group Addition Law on an Elliptic Curve

There is a one-to-one correspondence between the points over a finite field $E/\mathbb{F}_p$ and over $E/\mathbb{P}^2$, which can be used to formulate the addition law algebraically.

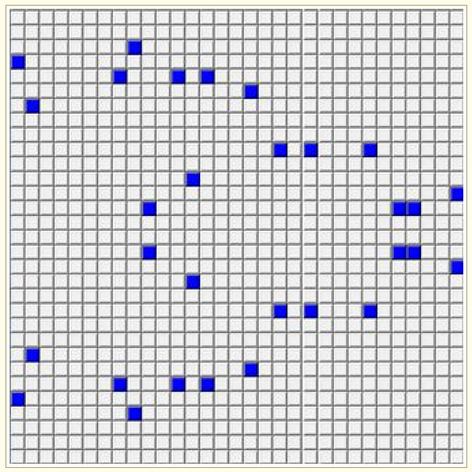

Figure 2: $E : y^2 = x^3 + x + 16$ over $\mathbb{F}_{31}$

The number of points on $E/\mathbb{F}_p$ is always in the Hasse interval

$$\mathcal{H}_p = [p + 1 - 2\sqrt{p},\ p + 1 + 2\sqrt{p}].$$

It is a classical result that if $q \in \mathcal{H}_p$ is a prime, then $p \in \mathcal{H}_q$.

Elliptic Pairs and Elliptic Reciprocity

Definition

An **elliptic pair** is an ordered pair of primes $(p, q)_d$ such that there exists an elliptic curve over $E/\mathbb{F}_p$ with order q that has complex multiplication (CM) in $\mathbb{Q}(\sqrt{-d})$, where $d \equiv_8 3$ is a square-free positive integer.

The Law of Elliptic Reciprocity

If $(p, q)_d$ is an elliptic pair, then so too is $(q, p)_d$.

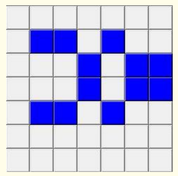

Figure 3: The curve $E : y^2 = x^3 + 3$ over $\mathbb{F}_7$ (plus $\mathcal{O}$, not shown) demonstrates that $(7, 13)_3$ is an elliptic pair.

Theorem

Let $(p, q)_d$ be an elliptic pair. Then if $d = 3$, there exist unique integers a, b such that $p = a^2 + 3b^2$ and $q = p + 1 + a - 3b$. If $d \neq 3$, there exist integers a, b such that $4p = a^2 + db^2$ and $q = p + 1 + a$.

Theorem

Let $(p, q)_d$ be an elliptic pair with $p < q$ and $d \neq 3$. If $4p = a^2 + db^2$ $(a, b > 0)$, then $4q = (a + 2)^2 + db^2$.

If $q \in \mathcal{H}_p$, then a curve $E/\mathbb{F}_p$ of order q exists with CM in $\mathbb{Q}(\sqrt{-d})$ for at most one $d \neq 3$, so $(p, q)_d$ is an elliptic pair for at most two values of d.

Elliptic Lists and Cycles

Definition

An **elliptic list (of length n)** is an ordered n-tuple of distinct primes $[p_1, p_2, ..., p_n]_d$ such that $(p_1, p_2)_d, (p_2, p_3)_d, ..., (p_{n-1}, p_n)_d$ are all elliptic pairs.

Definition

An **elliptic cycle (of length n)** is an ordered n-tuple of distinct primes $(p_1, p_2, ..., p_n)_d$ such that $[p_1, p_2, ..., p_n]_d$ is an elliptic list and $(p_n, p_1)_d$ is an elliptic pair.

Theorem

Let $\mathcal{L}(d) : \{d \in \mathbb{N} : d \equiv_4 3\} \to \mathbb{N}$ be the length n of the longest elliptic list over d. Then $\mathcal{L}(3) = 6$ and when $d \neq 3$, $\mathcal{L}(d) < \min(\{\text{primes } m : \left(\frac{-d}{m}\right) \neq -1\})$.

Theorem

There are no proper elliptic cycles of length $n > 2$, except in the case that $d = 3$ and $n = 6$.

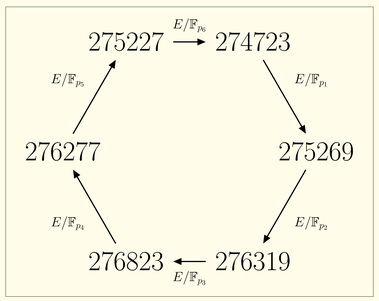

Figure 4: An elliptic 6-cycle, generated by the curve $E : y^2 = x^3 + 15$.

Cryptographic Applications

- Given a generator P of the points on E/K and a fixed point Q, it is generally difficult to find a value k such that $Q = kP = P + \cdots + P$.
- This problem is called the Elliptic Curve Discrete Logarithm Problem (ECDLP), and its one-way computational difficulty gives rise to a method of Diffie-Hellman key exchange, making elliptic curves useful for public-key cryptography.
- Due to attacks on DLP such as Silver - Pohlig - Hellman, it is necessary to find elliptic curves of prime order to achieve maximal security.

Future Work

- We can extend the group law into a ring law by defining multiplication on an elliptic curve. Is there an efficient way to compute this?
- For any given d, are there infinitely many elliptic pairs? If so, what is their distribution?
- Can we use the properties of elliptic pairs to generate elliptic curves of prime order more efficiently?
- How is the function $\mathcal{L}(d)$ related to the class number $h(-d)$?
- Is $\mathcal{L}(d)$ unbounded as $d \to \infty$?

References

[1] Silverberg, "Group order formulas for reductions of CM elliptic curves," *Contemporary Mathematics*, **521** (2010), pp. 107-120.

[2] Silverman and Stange, "Amicable Pairs and Aliquot Cycles for Elliptic Curves," *Experimental Mathematics*, **20:3** (2011), pp. 329-357.

Acknowledgments

Funding for this project was provided by the National Science Foundation under Award DMS 1062857 and by Boise State University.